LiTH, Linköpings tekniska högskola
IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2010-06-08
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
David Byers, 013-282821

Instructions
There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. The questions are grouped pair-wise under their corresponding topic.

You may answer at most 3 general questions and 3 in-depth questions. You may answer both the general and the in-depth question for at most one topic. If you answer more than 3 general or 3 in-depth questions, we will randomly discard excess answers. If you answer both questions for more than one topic, we will randomly discard answers for all but one of the affected topics.

You may answer in Swedish or English.

Grading
A correct answer for a general question gives you 2 points, and a correct answer for an in-depth question gives you 6 points. To pass the exam you need to accumulate at least 3 points from general questions and 9 points from in-depth questions. The exam grading depends on the total number of accumulated points.

The following grading scale is preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required	12	17	21

System Security

G1 What is the purpose of an integrity policy? Give an example of a security model that can be used to implement an integrity policy.

D1 What is role-based access control (RBAC)? How does it relate to other models for access control? What are the rules that define RBAC (specify them as correctly as you can, and explain each one).

Identification and authentication, Biometric user authentication

G2 Fingerprints is probably the most popular biometric method used in practice right now. Very high security applications tend, however, to use iris scan. Compare these two methods for at least two of the seven characteristics that should be considered when choosing a biometric method. The characteristics chosen in your comparison should explain why fingerprints are so popular while iris scan is regarded as better suited to high security requirements.

D2 Neither biometric measurements nor tokens can easily be falsified if properly designed. The course presents, however, some risks for such an event. Discuss a specific attack on a token and a specific attack on some biometric characteristic and compare the resources and skill needed in each case! Then include the general risks and drawbacks with tokens versus biometrics as such in your discussion! Give your personal final evaluation of which of your two examples that you regard as most secure, the token or the biometric!

Network security

G3 Explain what a trust relationship is, and why trust relationships are so important in network security.

D3 AUSCERT defines the term "security domain" as "a network of computer systems that share a specified security level through a common element". Explain why security domains are such an important concept when designing secure computer networks. Explain how security domains relate to security mechanisms. Explain why overlapping security domains could be a problem from a security point of view. Give at least two real world examples of security domains.

Risk analysis

G4 What is the typical output of a risk analysis?

D4 Explain the Risk Management Framework (RMF) and explicitly state in which stage of the RMF a risk analysis would be performed.

Business continuity planning, Physical security

G5 Explain and exemplify what a control is with regard to threats in physical security.

D5 Explain and exemplify the principles of breadth, depth and deterrence when planning a layered defense for physical security.